

DOCKET FILE COPY ORIGINAL

RECEIVED

JUN 12 1998

FEDERAL COMMUNICATIONS COMMISSION
OFFICE OF THE SECRETARY

Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of)
)
Communications Assistance for) CC Docket No. 97-213
Law Enforcement Act)

To the Commission:

REPLY COMMENTS OF EPIC, EFF AND THE ACLU

Congress enacted the Communications Assistance for Law Enforcement Act ("CALEA") in response to concerns expressed by the FBI and law enforcement that technological developments in our country's telecommunications infrastructure were impeding law enforcement's surveillance capabilities. In Section 103(a) of CALEA, Congress enumerated four capability requirements that telecommunications carriers must meet. These four requirements represent "both a floor and a ceiling" on the capability requirements that may be imposed on carriers.^{1/} Any capability requirement that falls outside the requirements of Section 103(a) may not be included in a "safe harbor" standard adopted by either industry or the Commission.

The comments filed in this proceeding are striking in their near unanimous opposition to including the FBI's punch list items in the safe harbor standard. With the exception of the FBI, all parties agree that the FBI's punch list items exceed the capability requirements of Section 103(a). These comments amply demonstrate that requiring carriers to provide the punch list capabilities would violate the "ceiling" established by Section 103(a).

^{1/} See H.R. Rep. No. 103-827 at 22.

No. of Copies rec'd
List A B C D E

054

The interim standard adopted by the Telecommunications Industry Association ("TIA") also violates the "ceiling" established by Section 103(a), and accordingly must be rejected as "deficient" under Section 107(b). Specifically, the requirement that wireless services providers provide location tracking information exceeds the capability requirements mandated by CALEA. That the industry may not oppose the inclusion of the location tracking capability requirement in a safe harbor standard does not render that standard compliant with CALEA.

Several commenters acknowledge that the industry included the location tracking requirement in the interim standard as a "compromise" to law enforcement's demands for extensive location information.^{2/} Further, several commenters concede that the location tracking requirement exceeds the scope of CALEA.^{3/} Indeed, even TIA notes that the interim standard was industry's attempt to reach a "consensus" with the FBI, even though industry believed that many of the FBI's demands were not mandated by CALEA.^{4/} TIA further acknowledges that location information may not fall within

^{2/} See, e.g., Comments of AT&T at 13 ("[Location information] was included in the standard at the beginning and end of a wireless call as a compromise to law enforcement's much broader claim that CALEA required carriers to provide such information whenever a wireless phone registered automatically or as it moved from cell site to cell site."); Comments of USTA at 2-3 ("[The interim standard] includes features, such as location tracking . . . , which the industry believed were beyond the scope of CALEA, but which were insisted upon by law enforcement."); Comments of Personal Communications Industry Association at 3; Comments of Bell South ("While location arguably falls outside of the strict definition of call identifying information, the [interim] standards organization agreed to provide location [information] . . . as an accommodation to law enforcement.").

^{3/} See *id.*; see also Comments of AT&T at 13 ("AT&T agrees that location information was not required under CALEA.").

^{4/} Comments of TIA at 11.

the definition of call-identifying information as "location information is not dialing or signaling information."^{5/}

Despite acknowledging that location tracking information falls outside the capability requirements of Section 103(a), TIA and other industry members support the interim standard. The industry, however, cannot raise the ceiling established by CALEA any more than the FBI or the Commission. The industry on its own, subject to other procedural and substantive limitations on electronic surveillance imposed by CALEA and Title III, may implement capabilities that will allow law enforcement access to location information, but those capabilities cannot be mandated pursuant to CALEA.

The interim standard is also deficient in that it fails to protect privacy interests in packet-switched communications.^{6/} The interim standard does not require carriers to separate call content and call-identifying information for packet-switched communications. Accordingly, under the interim standard, law enforcement would be eligible to obtain the full content of customer communications from carriers using packet switching even when the government is only authorized to intercept addressing or signaling data. As the Commission knows well, the growing use of packet switching in all networks, as represented by Sprint's announcement just this week, illustrates the need to have full privacy protections applied to packet-switched networks.

^{5/} Comments of TIA at 76.

^{6/} Congress specifically granted the Commission authority to set technical requirements or standards as a means to protect the privacy interests of telecommunications users. Section 107(b) allows any party who believes the industry's standards to be "deficient," to petition the Commission to establish standards that "protect the privacy and security of communications not authorized to be intercepted."

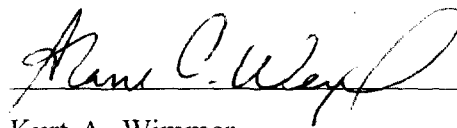
Section 107(b)(2) authorizes the Commission to "protect the privacy and security of communications not authorized to be intercepted." Clearly, separating call content from call-identifying information for packet-switched communications would protect the privacy and security of such communications where law enforcement is authorized only to intercept call-identifying information. Yet the record before the Commission is devoid of any justification as to why the interim standard failed to include this privacy protection. For this reason, the interim standard should be found to be defective, and the issue of separating call content from call-identifying information for packet-switched communications should be addressed in an open forum.

* * *

To ensure that a "safe harbor" standard adopted pursuant to CALEA does not exceed the capability requirements in Section 103(a) and adequately protects privacy interests, the Commission should implement a notice and comment rulemaking proceeding to develop such a standard. Section 107(b) authorizes the Commission "to establish" a standard, it does not authorize the Commission to delegate this responsibility to another entity. Moreover, remanding the standard-setting process to TIA likely would again produce a "compromise" between industry and law enforcement that fails to protect the privacy interests of telecommunications users. So that all interested parties may fully participate in the implementation of CALEA, the Commission should commence a rulemaking proceeding that follows the mandates of the Administrative Procedure Act. All parties participating in the rulemaking proceeding should be subject to the Commission's ex parte notification requirements.

The Commission's rulemaking proceeding should deal *de novo* with establishing the capability and technological requirements appropriately covered by CALEA. We urge the Commission to deny the FBI Petition, reject the industry's compromise standard and commence an independent proceeding to establish technical standards that satisfy the capability requirements and the privacy protections of CALEA.

Respectfully submitted,



Kurt A. Wimmer
Gerard J. Waldron
Alane C. Weixel
Ellen P. Goodman
Erin Egan

David L. Sobel, Esq.
Marc Rotenberg, Esq.
ELECTRONIC PRIVACY
INFORMATION CENTER
666 Pennsylvania Avenue, S.E.
Suite 301
Washington, D.C. 20003

COVINGTON & BURLING
1201 Pennsylvania Avenue, N.W.
P.O. Box 7566
Washington, D.C. 20044-7566
202-662-6000
Attorneys for EPIC, EFF and the ACLU

Barry Steinhardt, Esq.
President
ELECTRONIC FRONTIER
FOUNDATION
1550 Bryant Street
Suite 725
San Francisco, California 94103

Mark J. Emery
Technical Consultant
3032 Jeannie Anna Court
Oak Hill, Virginia 21071

Laura Murphy, Esq.
Cassidy Sehgal
AMERICAN CIVIL LIBERTIES UNION
122 Maryland Avenue, N.E.
Washington, D.C. 20002

June 12, 1998